

**Notice of Allowability**

Application No.

10/671,319

Examiner

Ronald Baum

Applicant(s)

DELANY, MARK

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 6/24/05.
2. ☒ The allowed claim(s) is/are 1-29.
3. ☒ The drawings filed on 23 September 2002 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some\* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).


\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of: \_\_\_\_\_
- Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit  
of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413),  
Paper No./Mail Date \_\_\_\_\_
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

### EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with John W. Branch, Reg. No. 41,633 on 7/21/2005.

1. **Replace** claims 1,5-8,19-24,28, and 29 with:

1. A method for message authentication, comprising:

generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name server (DNS) that is associated with the domain;

employing a message server associated with the domain to employ a private component of the key pair to digitally sign the message;

employing a message server associated with a domain of a recipient to verify the domain of origination for the message with the public component of the key pair;

if a message originates from a sender's address associated with the domain, employing the private component of the key pair to digitally sign the message and forwarding the digitally signed message towards the recipient of the message; and

if the public component stored with the DNS verifies that the digitally signed message originated from the domain associated with the sender's address, providing the verified digitally signed message to the recipient.

5. The method of Claim 1, wherein the message server includes a mail server associated with the domain to forward the digitally signed message towards the recipient of the message.

6. The method of Claim 1, wherein the message server includes a mail server associated with the domain to employ the private component of the key pair to digitally sign the message.

7. The method of Claim 1, wherein the message server includes a mail server that is associated with the domain of the recipient to verify the domain of origination for the message with the public component of the key pair.

8. The method of Claim 1, wherein the message server includes a mail server that is associated with the domain of the recipient to provide the verified digitally signed message to the recipient.

19. A processor readable medium of tangibly embodied software that enables actions for message authentication, comprising:

generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name server (DNS) that is associated with the domain;

enabling a message server associated with the domain to employ a private component of the key pair to digitally sign the message;

enabling a message server associated with a domain of a recipient to verify the domain of origination for the message with the public component of the key pair;

if a message originates from a sender's address associated with the domain, employing the private component of the key pair to digitally sign the message and forwarding the digitally signed message towards the recipient of the message; and

if the public component stored with the DNS verifies that the digitally signed message originated from the domain associated with the sender's address, providing the verified digitally signed message to the recipient.

20. The processor readable medium of Claim 19, further comprising generating a selector that is associated with the key pair, wherein the selector is employable to identify the key pair's public component for accessing by the DNS.

21. The processor readable medium of Claim 19, further comprising generating a plurality of key pairs associated with the domain, wherein at least two key pairs are associated with at least two different senders and wherein each public component of each key pair is accessible by the DNS associated with the domain.

22. The processor readable medium of Claim 21, further comprising separately associating private components of the at least two key pairs with at least two mail servers, wherein the at least two mail servers are associated with the domain.

23. The processor readable medium of Claim 21, wherein each private component of each key pair employs a mail server associated with the domain to forward the digitally signed message towards the recipient of the message.

24. A client that enables message authentication, comprising:

a first component for originating a message for communication by a message server associated with a domain, wherein a key pair is associated with the domain, wherein a public component of the key pair is accessible to a domain name server (DNS) that is associated with the domain;

a second component for enabling the message server associated with the domain to employ a private component of the key pair to digitally sign the originated message;

a third component for enabling a message server associated with a domain of a recipient to verify the domain of origination for the message with the public component of the key pair;

if a message originates from a sender's address associated with the domain, a fourth component that provides for enabling a private component of the key pair to be employed to digitally sign the message and forwarding the digitally signed message towards a recipient of the message; and

if the public component stored with the DNS verifies that the digitally signed message originated from the domain associated with the sender's address, a fifth component for providing the verified digitally signed message to the recipient.

28. A message server that enables message authentication, comprising:

a first component for enabling the generation of a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name server (DNS) that is associated with the domain;

wherein the message server is associated with the domain and employs a private component of the key pair to digitally sign a message that is originated with the message server;

a second component for enabling a message server associated with a domain of a recipient to verify the domain of origination for the message with the public component of the key pair;

if a message originates from a sender's address associated with the domain, a third component for enabling a the private component of the key pair to be employed to digitally sign the message and forwarding the digitally signed message towards the recipient of the message; and

if the public component stored with the DNS verifies that the digitally signed message originated from the domain associated with the sender's address, a fifth component for providing the verified digitally signed message to the recipient.

29. A method for enabling message authentication, comprising:

means for enabling the generation of a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name server (DNS) that is associated with the domain;

means for employing a message server associated with the domain to employ a private component of the key pair to digitally sign the message;

means for employing a message server associated with a domain of a recipient to verify the domain of origination for the message with the public component of the key pair;

if a message originates from a sender's address associated with the domain, means for enabling a private component of the key pair to be employed to digitally sign the message and forwarding the digitally signed message towards a recipient of the message; and

if the public component stored with the DNS verifies that the digitally signed message originated from the domain associated with the sender's address, means for providing the verified digitally signed message to the recipient.

*Examiner's Statement of Reasons for Allowance*

3. Claims 1-29 are allowed over prior art.
4. This action is in reply to applicant's correspondence of 24 June 2005
5. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.
6. As per claims 1, 14, 19, 24, 28, 29, generally, prior art of record, Gupta et al, U.S. Patent 6,389,532, fails to teach, alone, or in combination, at the time of the invention, of (claim 1 by example);

(Claim 1) A method for *message authentication*, comprising:

*generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name server (DNS) that is associated with the domain;*

*employing a message server associated with the domain to employ a private component of the key pair to digitally sign the message;*

*employing a message server associated with a domain of a recipient to verify the domain of origination for the message with the public component of the key pair;*

*if a message originates from a sender's address associated with the domain,*



employing the *private component* of the key pair to digitally *sign*  
*the message* and  
*forwarding* the digitally *signed message* towards *the recipient* of  
the message; and  
*if* the *public component* stored with the *DNS* *verifies* that the digitally  
*signed message* originated from the domain associated with the sender's address,  
*providing* the *verified* digitally *signed message* to the recipient.

7. The italicized above claim elements dealing with (again, by example; claim 1) "...  
*message authentication, ... generating a key pair associated with a domain, ... public component*  
*... domain name server ... associated with the domain; ... message server associated with the*  
*domain ... private component ... sign the message; ... message server associated with a domain*  
*of a recipient to verify the domain of origination ... if a message originates from a sender's*  
*address associated with the domain, ... private component ... sign the message ... forwarding ...*  
*signed message towards the recipient ... if ... public component ... DNS verifies ... signed*  
*message originated from the domain associated with the sender's address, providing ... verified*  
*... signed message to the recipient.*" serving to patently distinguish the invention from prior art.

Specifically, while the use of network based authentication and associated cryptographic content encryption, or parts thereof, for the purpose of providing secure electronic message transfer and general content security, is known in the prior art (i.e., see "Mercer, Alan, "Configuring Watchguard Proxies: Guideline to Supplementing Virus Protection and Policy Enforcement", Sept 5, 2003, SANS Institute, entire document, <http://www.securitytechnet.com/resource/rsc-center/vendor-wp/watchguard/1255.pdf>" for the case of general malware addressed issues (i.e., viruses), and inclusive of email (i.e., spam. etc.,)/electronic messaging

Art Unit: 2136

issues.), the use of network based cryptographic techniques (i.e., public key based) and services (i.e., authentication of network messages/email elements), with the further specificity of the use of device specific network nodes (the DNS) to verify the integrity of the message domain for the authenticated electronic messaging, is patently distinct in the art. More specifically, the “courser grained” approach of the claimed invention to using the domain of the electronic message originating domain, so that subsequent verification at the destination messaging server prior to forwarding of the signed/encrypted message to the recipient network node for further content/routing filtering (i.e., spam filtering of source email address), is not taught in the art at the time of the invention.

As per the applicants arguments in the previous remarks in the Amendment (of 24 June 2005), the examiner finds the applicant’s arguments to be persuasive in that the art of record does not teach or suggest the use of OSI application level aspects of message authentication where the electronic messaging/DNS aspects of the claimed invention apply, as described above, let alone provide a motivation to combine such elements, so as to therefore patently distinguish the invention from the prior art of record, other than from hindsight.

However, the claim language clearly associates the applicant’s invention to the use of source and destination network domain message servers that utilize specifically a public key based cryptographic signing authentication via an associated DNS (as interpreted by the examiner using the accepted definition “... A computer that can answer Domain Name Service (DNS) queries. The DNS server keeps a database of host computers and their corresponding IP addresses. Presented with the name apex.com, for example, the DNS server would return the IP address of the hypothetical company Apex. ... [Microsoft Press, “Computer Dictionary”, 3rd edition, 1997,

Art Unit: 2136

Microsoft Corporation, page 155]”), and associated signed message, versus; the use of lower OSI level cryptographic/authentication techniques that allow simple node to node (i.e., non-DNS, simple gateway/router, or non-third party network node) electronic messaging authentication.

8. Dependent claims 2-13, 15-18, 20-23, and 25-27 are allowable by virtue of their dependencies.


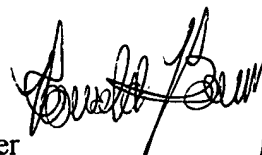
*Conclusion*

9. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum  
Patent Examiner



AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100